Authenticated Multiparty Secret Key Sharing Using Quantum Entanglement Swapping

Muneer Alshowkan, Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

In this poster we propose a new protocol for multiparty secret key sharing by using quantum entanglement swapping. Quantum Entanglement swapping is a process that allows two non-interacting quantum systems to be entangled. Further, to increase the security level and to make sure that the users are legitimate, authentication for both parties will be required by a trusted third party. In this protocol, a trusted third party will authenticate the sender and the receiver and help them forming a secret key. Furthermore, the proposed protocol will perform entanglement swapping between the sender and the receiver. The result from the entanglement swapping will be an Einstein-Podolsky-Rosen (EPR) pair that will help them in forming and sending the secret key without having the sender to send any physical quantum states to the receiver. This protocol will provide the required authentication of all parties to the trusted party and it will provide the required secure method in transmitting the secret key

Introduction

- **Bell States**

The canonical basis consist of only one single qubit such as:

$$\{|0\rangle, |1\rangle\}$$

Bell states which also called EPR (Einstein-Podolsky-Rosen) pairs consist of two entangled qubits in a noncanonical basis as:

$$\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$$

The Bell basis consists of four entangled vectors as follow

$$\frac{|\Psi^+\rangle = |01\rangle + |10\rangle}{\sqrt{2}}$$

$$\frac{|\Psi^-\rangle = |01\rangle - |10\rangle}{\sqrt{2}}$$

$$\frac{|\Phi^+\rangle = |00\rangle + |11\rangle}{\sqrt{2}}$$

$$\frac{|\Phi^-\rangle = |00\rangle - |11\rangle}{\sqrt{2}}$$

Forming Bell basis in two-dimensional case requires applying Hadamard matrix which performs the following:

$$|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Applying song input in the circuit in Fig 1. result in creating one of Bell basis:

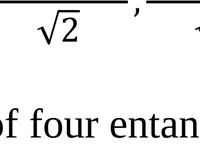

Fig 1. Quantum Circuit to Create Bell State

The result of each input create Bell Basis:

$$|00\rangle \rightarrow |\Phi^+\rangle, |01\rangle \rightarrow |\Psi^+\rangle, |10\rangle \rightarrow |\Phi^-\rangle, |11\rangle \rightarrow |\Psi^-\rangle$$

Proposed Algorithm

In this process we assume that each party shares N EPR pairs with the trusted party named Charlie and not sharing EPR pairs with the other parties. The first step in this protocol will be establishing an EPR-pair between the sender and the receiver by the help of the trusted node Charlie. After that Charlie will act as generator for EPR-pairs between the sender and the receiver to allow them to communicate with each other's. The first step require Charlie to help the sender (Alice) and the receiver (Bob) to form an EPR pair. The shared EPR pair between Alice and Charlie will be as follows:

$$AC = \frac{|0\rangle_A|0\rangle_C + |1\rangle_A|1\rangle_C}{\sqrt{2}}$$

And the shared EPR pair between Charlie and Bob is as follows:

$$CB = \frac{|0\rangle_C|0\rangle_B + |1\rangle_C|1\rangle_B}{\sqrt{2}}$$

After applying the entanglement swapping and depending on the result of Charlie's measurement, Alice and Bob can build their entangled qubits after applying Pauli-X, Pauli-Z, both or no gate. For the particles in Alice's and Bob's possessions, the result of the process will be one of the following EPR pairs:

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$$
$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$
$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$$
$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

After forming the EPR pair between Alice and Bob, they have the option to measure their EPR pair using one of the basis . When Alice measure her qubit (first qubit in the EPR pair) using one of these basis, Bob's qubit (second qubit in the EPR pair) will be collapsed to the opposite of the result of Alice's state. However, for Bob to have the correct opposite state, he needs to measure his qubit using the same basis Alice used to measure her qubit.

Alice can start to measure her qubit in one of these basis and get the measurement result. After that Alice can meet Bob on the classical channel and inform him about the basis she used in measuring her qubit without disclosing her measurement result. Then, Bob can measure his qubits using the same basis Alice used. The result of Bob's measurement will be the opposite of Alice's result in the same basis. For example:
Alice basis $|+\rangle, |-\rangle$ and her result is $|+\rangle$ then Bob's $|-\rangle$
Alice basis $|0\rangle, |1\rangle$ and her result is $|0\rangle$ then Bob's $|1\rangle$.

Conclusion

We have presented a multiparty quantum secret key sharing using quantum entanglement swapping. This protocol solves the problem of trust between sender and receiver. Where there will be a trusted third party who can authenticate each party to the other. Sender and receiver exchange data without having prior entangled state between. Also, quantum medium is not required and will take the advantage of quantum entanglement instead.